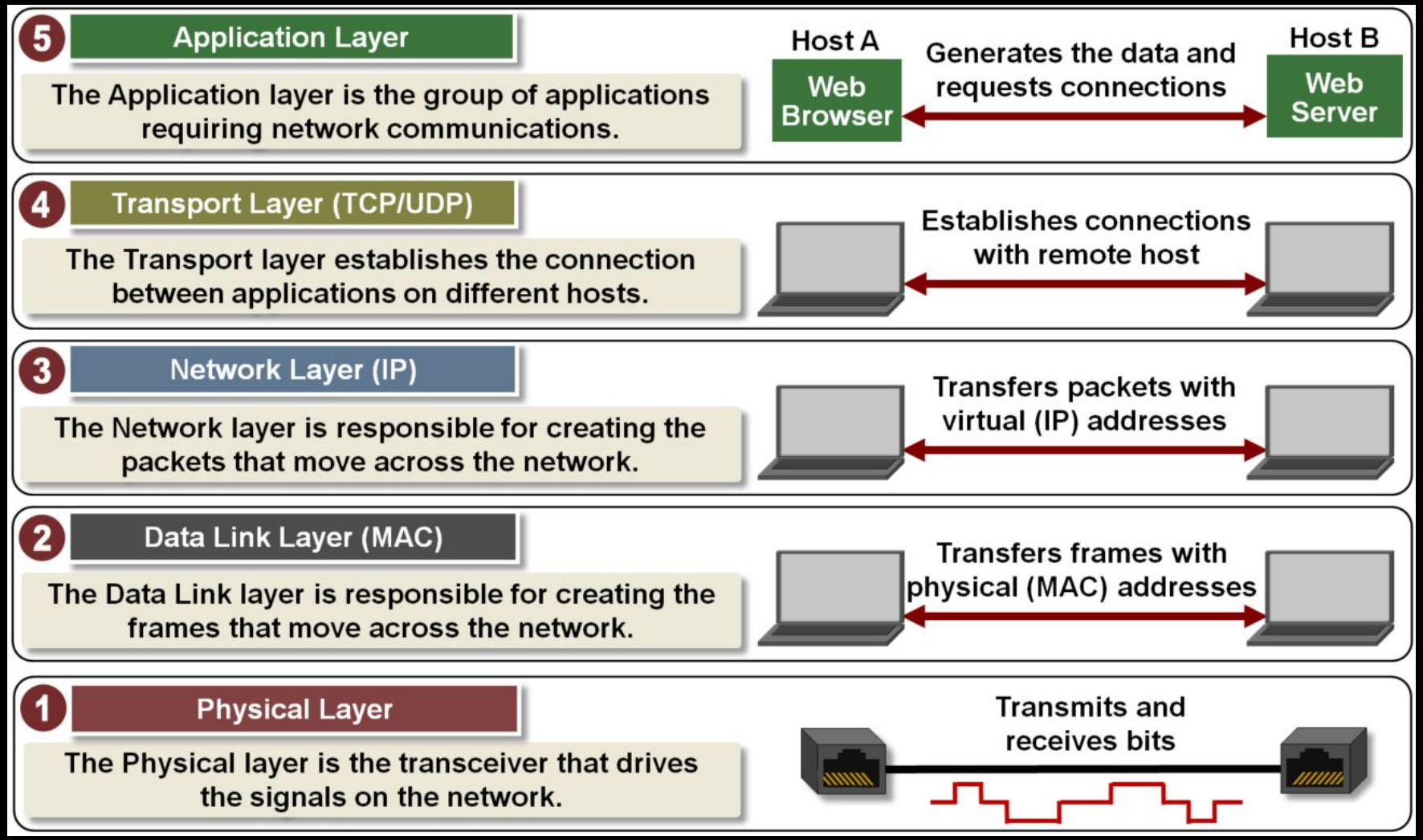
인공지능 보안

-07-

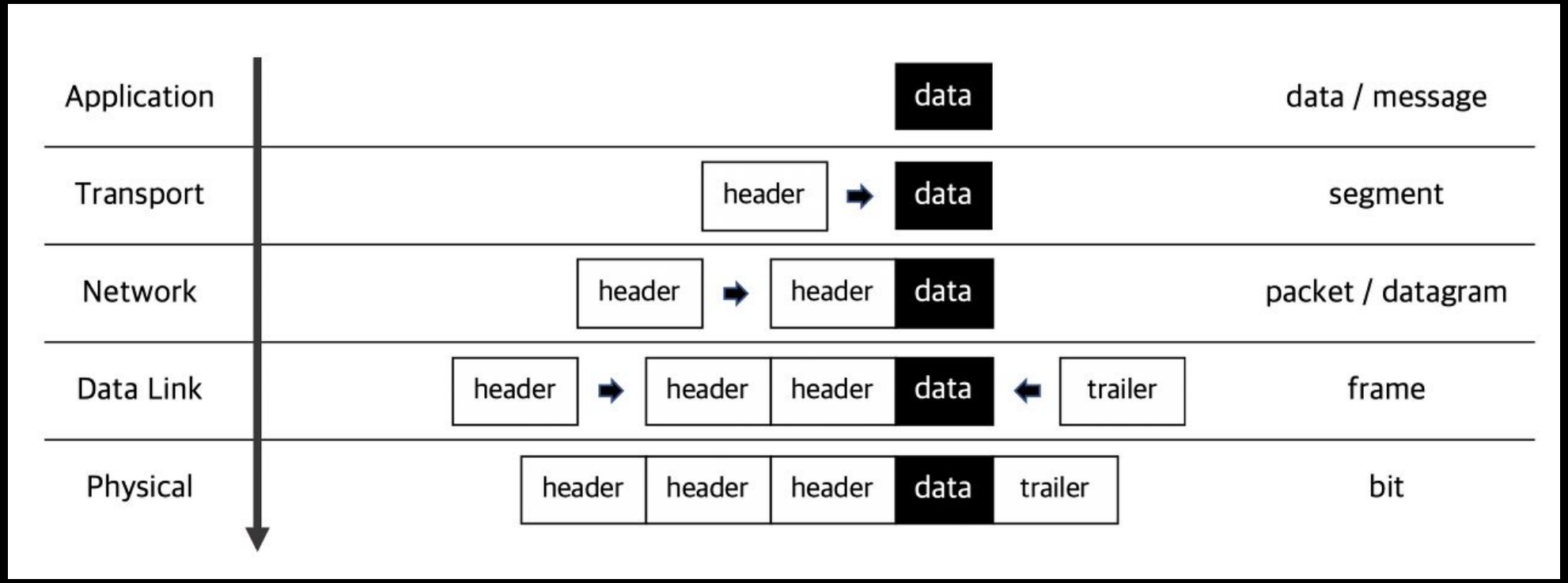
네트워크 보안

TCP/IP 계층

TCP/IP 계층


5
Application Layer
The Application layer is the group of applications requiring network communications.
Host A
Web Browser
Generates the data and requests connections
Host B
Web Server
4
Transport Layer (TCP/UDP)
The Transport layer establishes the connection between applications on different hosts.
Establishes connections with remote host
3
Network Layer (IP)
The Network layer is responsible for creating the packets that move across the network.
Transfers packets with virtual (IP) addresses
2
Data Link Layer (MAC)
The Data Link layer is responsible for creating the frames that move across the network.
Transfers frames with physical (MAC) addresses
1
Physical Layer
The Physical layer is the transceiver that drives the signals on the network.
Transmits and receives bits

TCP/IP 데이터 전송 흐름



DoS 공격

서비스 거부 공격(DoS)

- 다른 해킹에 비해 비교적 간단한 것으로 일종의 훼방
  - 예를 들면 깡패가 노점상의 장사를 방해하는 것
  - 집기를 부수거나 식재료의 공급을 끊거나 나쁜 재료를 몰래 섞는 것

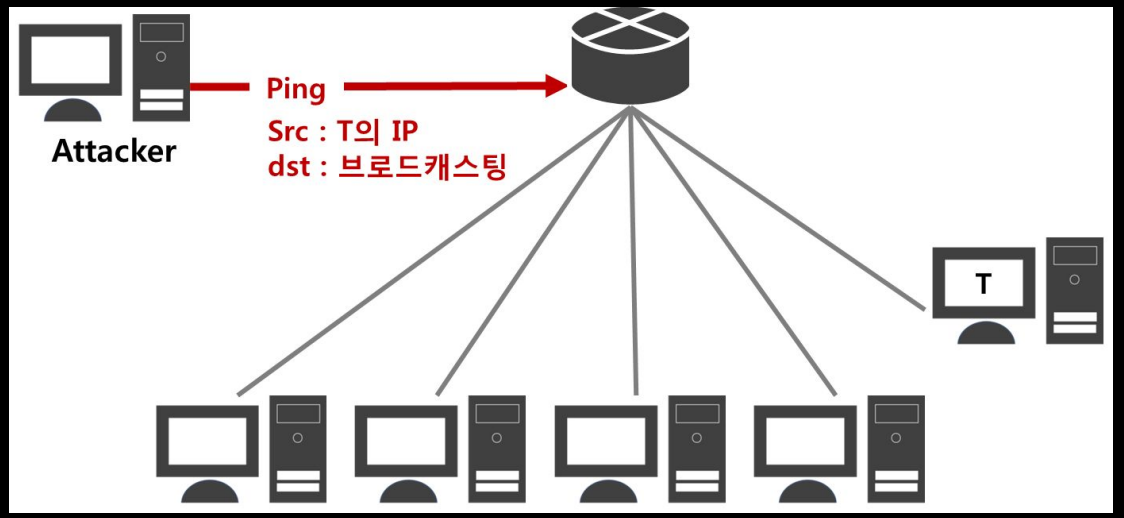
서비스 거부 공격(DoS)

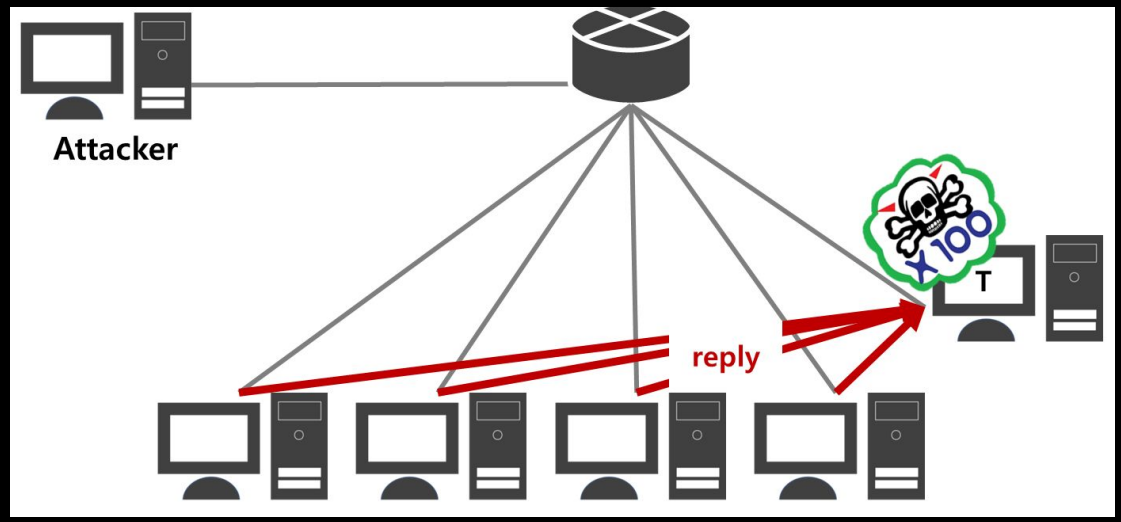
- 취약점 공격형
  - 특정 형태의 오류가 있는 네트워크 패킷의 처리 로직에 문제가 있을 때 공격 대상이 그 문제점을 이용하여 오작동을 유발하는 형태
  - 보잉크/봉크/티어드롭 공격, 랜드 공격 등
-
- 자원 고갈 공격형
  - 네트워크 대역폭이나 시스템의 CPU, 세션 등의 자원을 소모시키는 형태
  - 랜드 공격, 죽음의 핑 공격, SYN 플러딩 공격, HTTP GET 플러딩 공격, HTTP CC 공격, 동적 HTTP 리퀘스트 플러딩 공격, 슬로 HTTP 헤더 공격, 슬로 HTTP POST 공격, 스머프 공격, 메일 폭탄 공격 등

SMURF (ICMP Flooding)

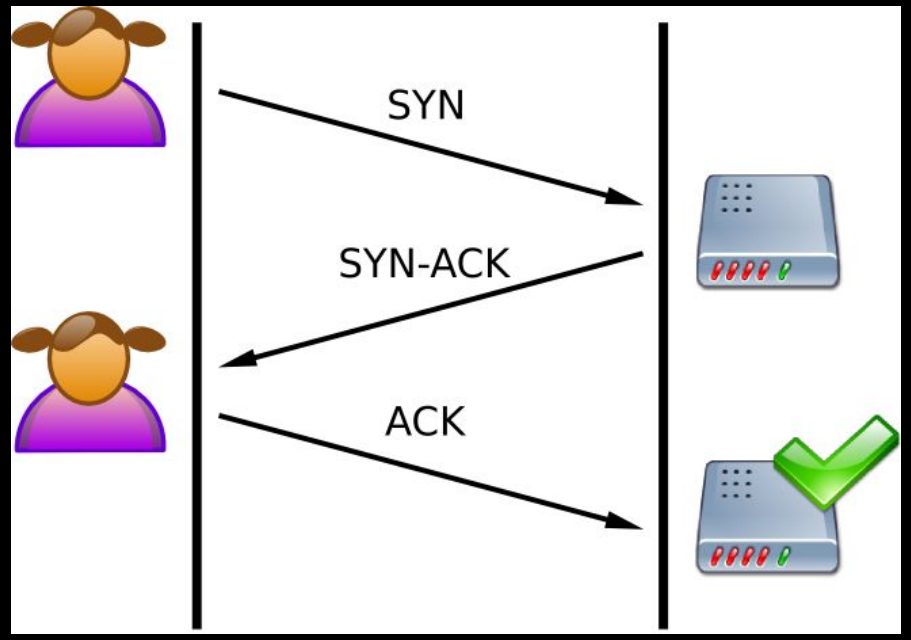
ICMP Protocol

SMURF (ICMP Flooding)

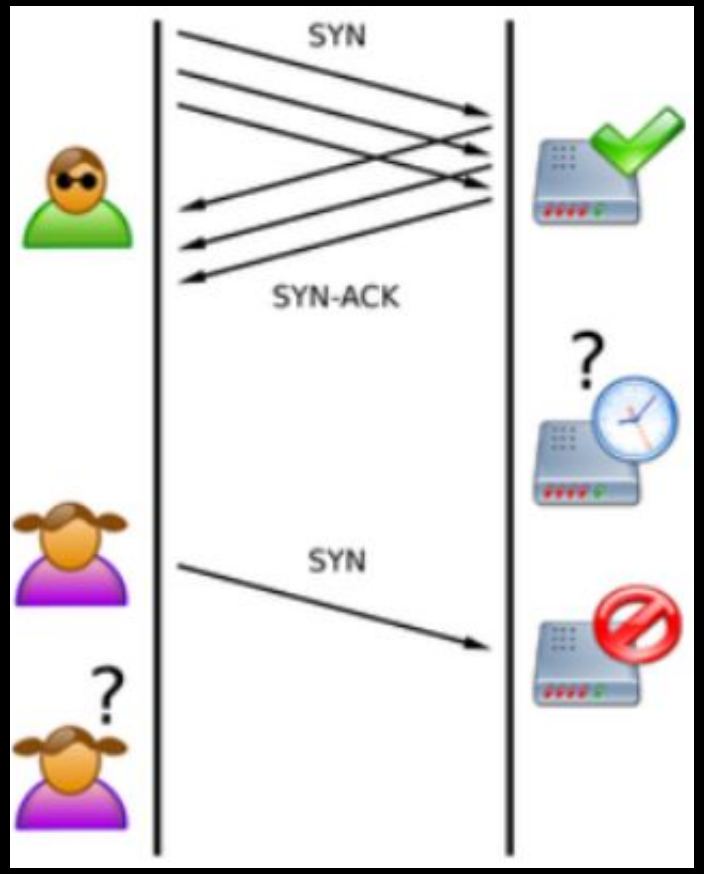




TCP SYN Flooding

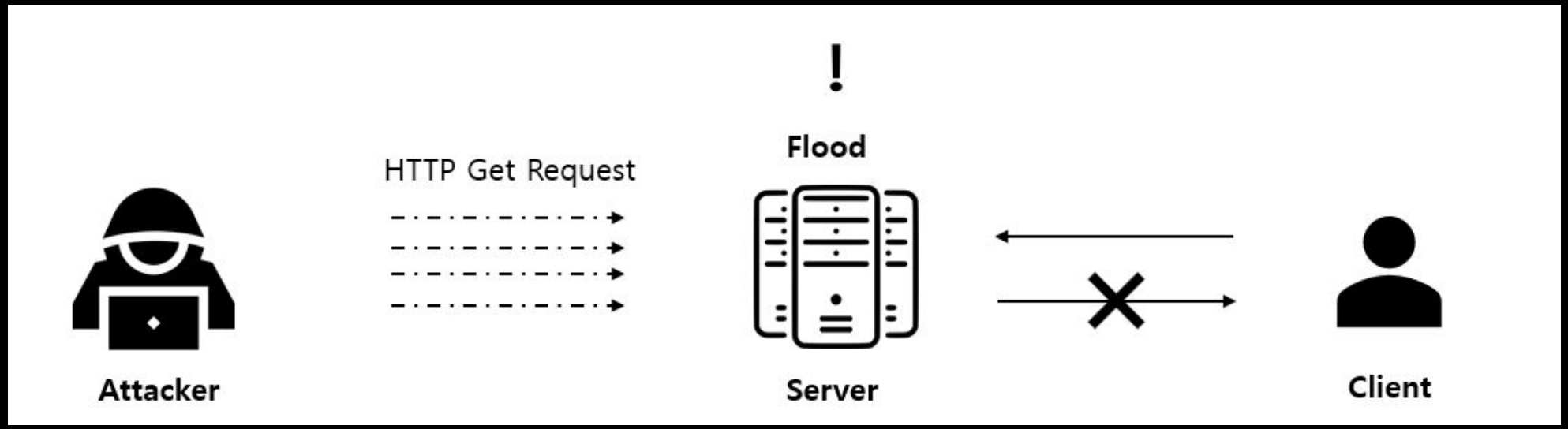


TCP Handshakes



TCP SYN Flooding

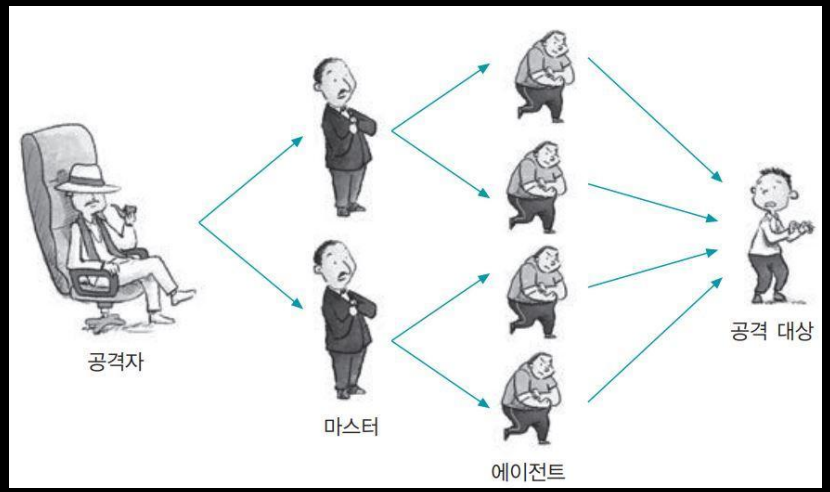
HTTP GET Flooding

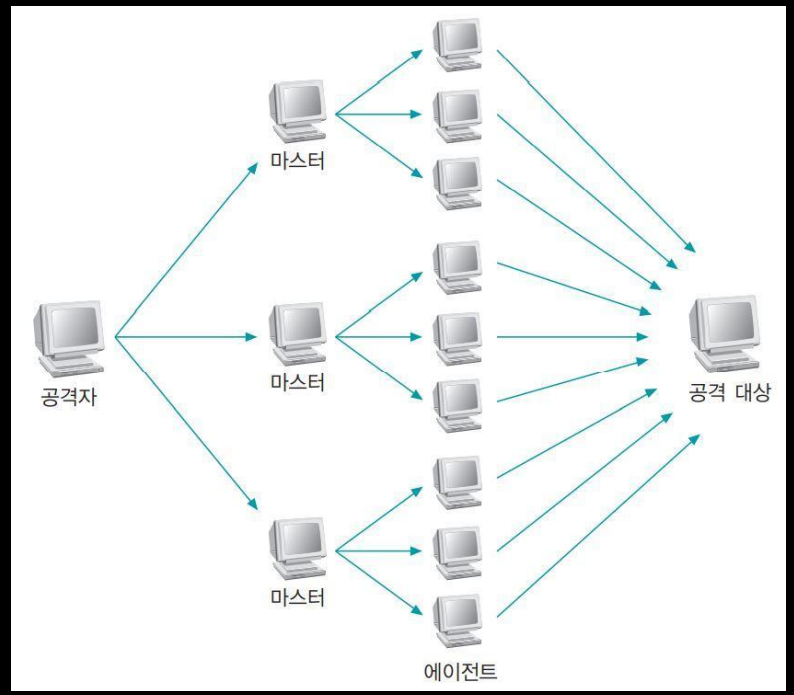


DDoS 공격

분산 서비스 거부 공격(DDoS)

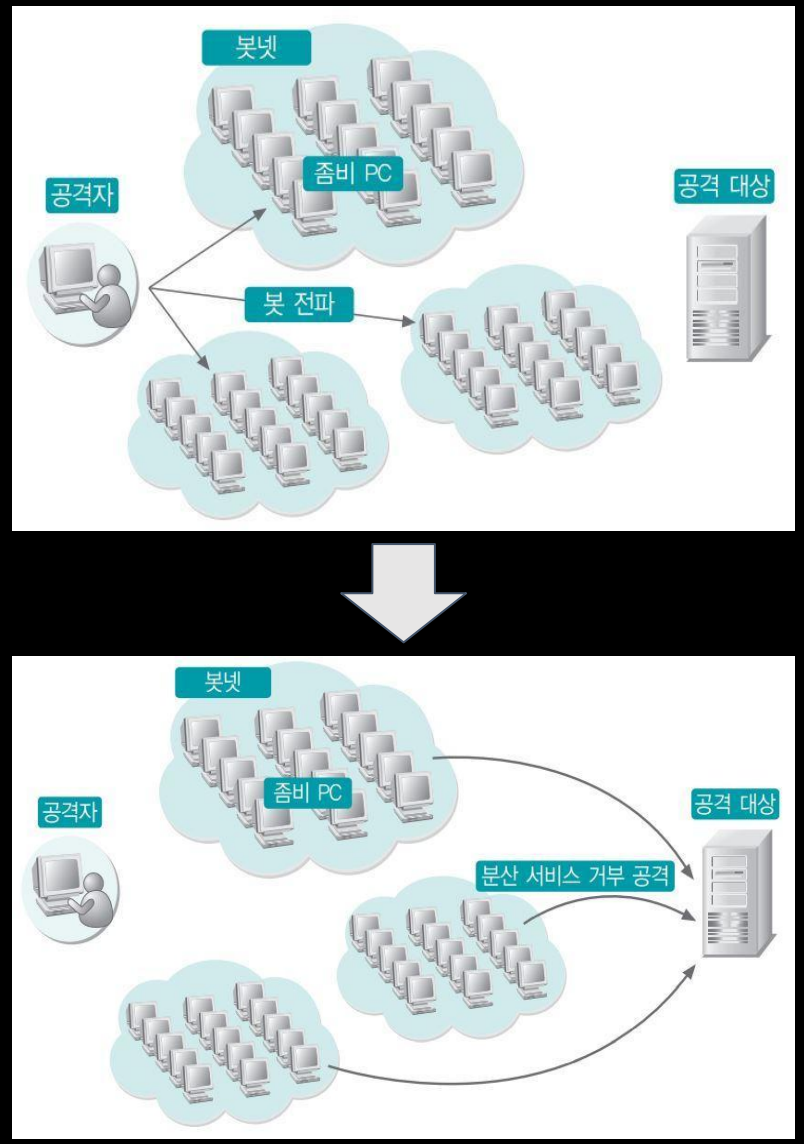
- 분산 서비스 거부 공격의 기본 구성
  - 구조는 폭력 조직과 비슷하여 공격자를 폭력 조직의 두목, 마스터를 행동대장, 에이전트를 졸개에 비유
  - 과거의 분산 서비스 거부 공격에서는 마스터와 에이전트가 중간자인 동시에 피해자





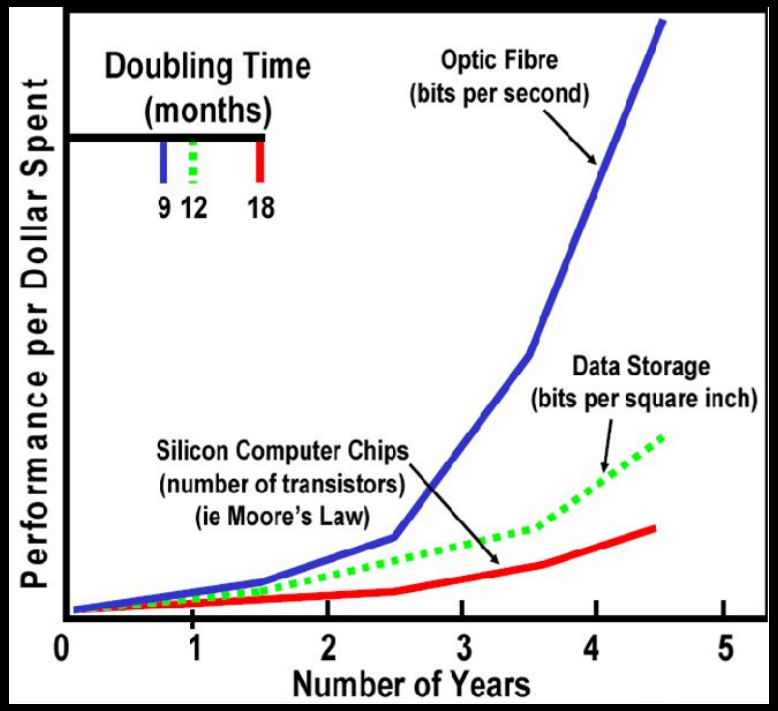
분산 서비스 공격 과정

- 최근에 발생하는 분산 서비스 공격 과정
  - PC에서 전파가 가능한 형태의 악성 코드를 작성
  - 분산 서비스 거부 공격을 위해 사전에 공격 대상과 스케줄을 정한 뒤 악성 코드에 코딩
  - 인터넷을 통해 악성 코드를 전파
    (봇: 분산 서비스 거부 공격에 사용되는 악성 코드)
    전파 과정에서는 별다른 공격 없이 잠복
    악성 코드에 감염된 PC를 좀비 PC라고 하며, 좀비 PC끼리 형성된 네트워크를 봇넷 이라고 함
  - 공격자가 명령을 내리거나 봇넷을 형성한 좀비 PC들이 정해진 공격 스케줄에 따라 일제히 공격 명령을 수행



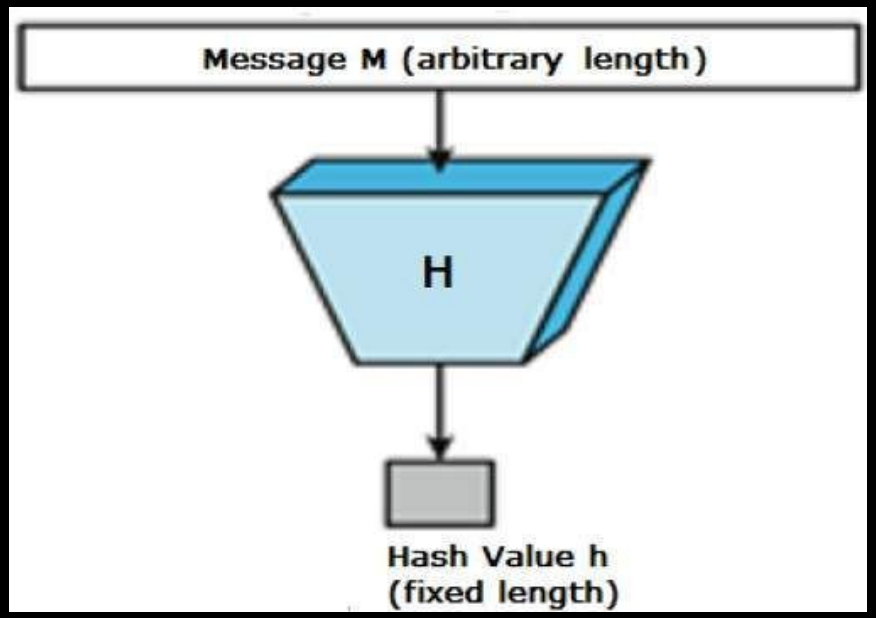
Hash

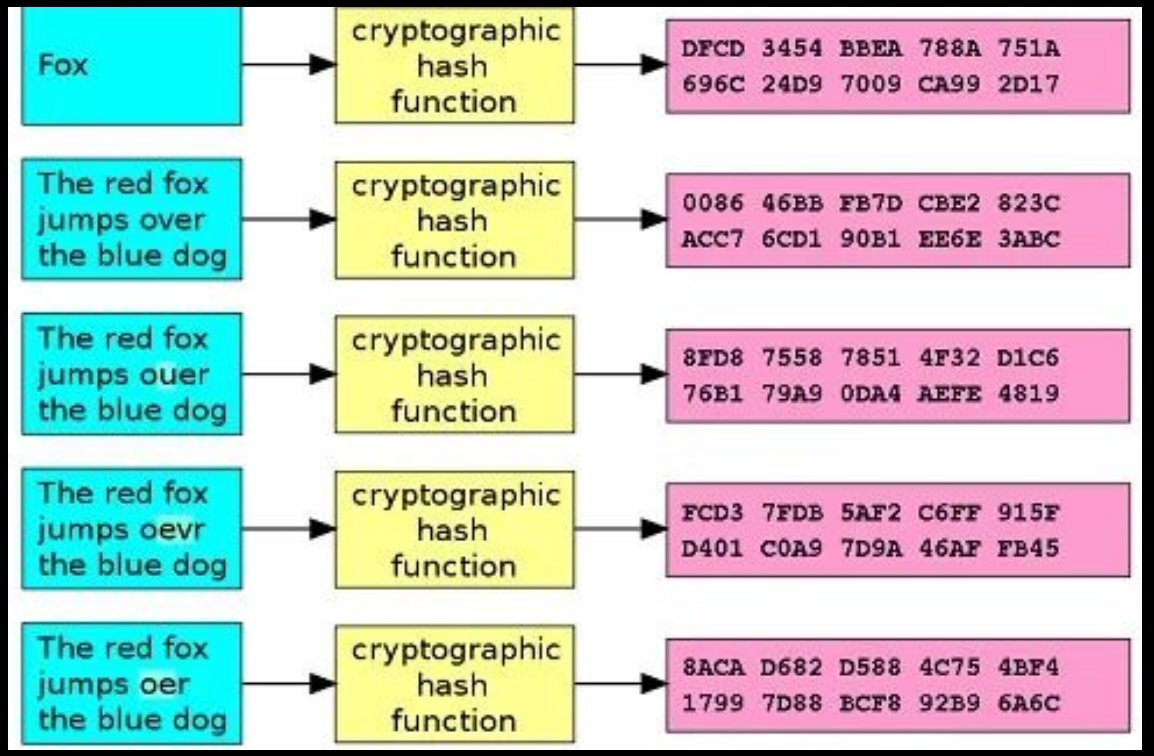
Security in High-speed Networks



Moore's law comparison between the increase expectations of the network bandwidth and storage capacity

Hash Function

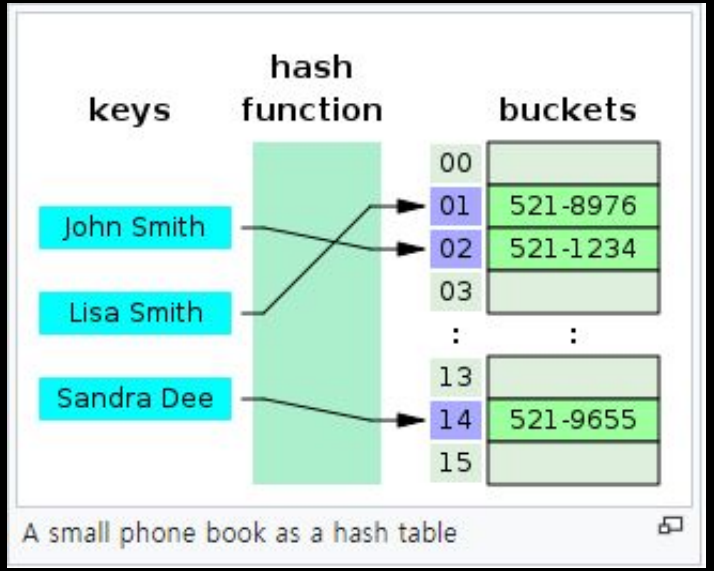




Hash Table

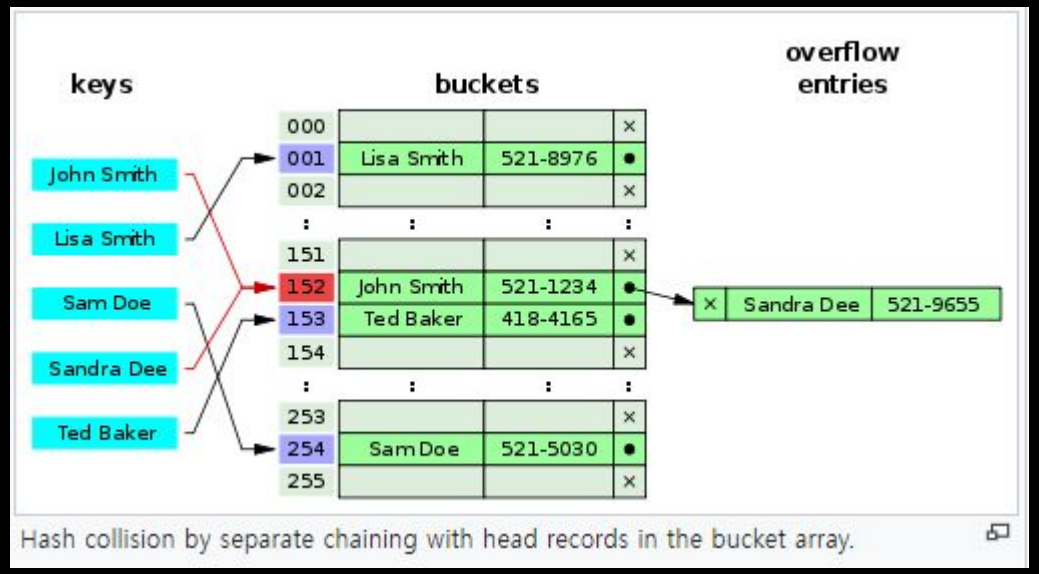
- The advantage of using hashing is that the table address of a record can be directly computed from the key

- Hash functions should provide a uniform distribution of hash values
- Cryptographic hash functions are believed to provide good hash functions for any table size, either by modulo reduction or by bit masking



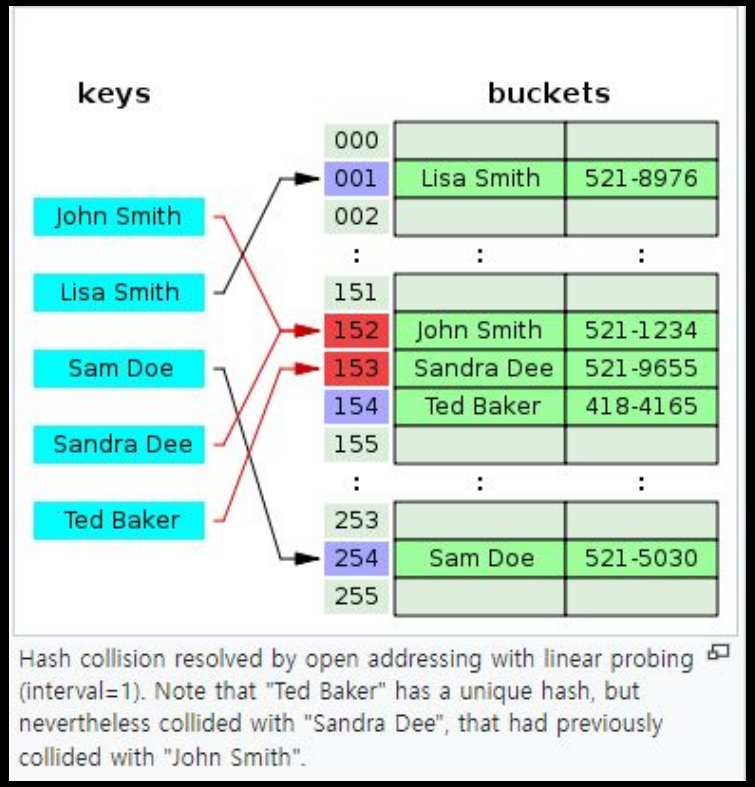
$$\text{Hash} = \text{Hash-Function(Key)}$$
$$\text{Index} = \text{Hash} \ \% \ \text{Hash-Table-Size}$$

Hash Table



Hash collision by separate chaining with head records in the bucket array.

Chaining



Hash collision resolved by open addressing with linear probing (interval=1). Note that "Ted Baker" has a unique hash, but nevertheless collided with "Sandra Dee", that had previously collided with "John Smith".

Open addressing

Q&A